J. Korean Math. Soc. **48** (2011), No. 6, pp. 1249–1268
http://dx.doi.org/10.4134/JKMS.2011.48.6.1249

8-RANKS OF CLASS GROUPS OF IMAGINARY QUADRATIC NUMBER FIELDS AND THEIR DENSITIES

Hwanyup Jung and Qin Yue

Abstract. For imaginary quadratic number fields $F = \mathbb{Q}(\sqrt{\varepsilon p_1 \cdots p_{t-1}})$, where $\varepsilon \in \{-1, -2\}$ and distinct primes $p_i \equiv 1 \bmod 4$, we give conditions of 8-ranks of class groups $C(F)$ of F equal to 1 or 2 provided that 4-ranks of $C(F)$ are at most equal to 2. Especially for $F = \mathbb{Q}(\sqrt{\varepsilon p_1 p_2})$, we compute densities of 8-ranks of $C(F)$ equal to 1 or 2 in all such imaginary quadratic fields F. The results are stated in terms of congruence relations of p_i modulo 2^n, the quartic residue symbol $(\frac{p_1}{p_2})_4$ and binary quadratic forms such as $p_2^{h_+(2p_1)/4} = x^2 - 2p_1 y^2$, where $h_+(2p_1)$ is the narrow class number of $\mathbb{Q}(\sqrt{2p_1})$. The results are also very useful for numerical computations.

1. Introduction

It is a classical topic to study the structure of 2-primary subgroups of the narrow class groups $C_+(F)$ for quadratic number fields F ([1, 2, 3, 9, 12, 13, 14]). Gerth gave a method to compute their densities ([4, 5, 6, 15, 16]). By genus theory, we have known 2-rank of $C_+(F)$; by Rédei's matrix, we have got 4-rank of $C_+(F)$ clearly. In this paper, we always assume that $F = \mathbb{Q}(\sqrt{\varepsilon p_1 \cdots p_{t-1}})$, where $\varepsilon \in \{-1, -2\}$, are imaginary quadratic number fields with distinct primes $p_i \equiv 1 \bmod 4$. We will mainly obtain conditions for 8-ranks of class groups $C(F)$ equal to 1 or 2 provided that 4-ranks of $C(F)$ are at most equal to 2. Especially for $F = \mathbb{Q}(\sqrt{\varepsilon p_1 p_2})$, we compute densities of 8-ranks of $C(F)$ equal to 1 or 2 in all such fields.

In §2, we describe some well-known facts. We support the degree 4 extension N_+ over $K = \mathbb{Q}(\sqrt{2p_1})$ with prime $p_1 \equiv 1 \bmod 8$, in which all finite primes of K are unramified. We set up relations between the Galois group $Gal(N_+/K)$ and the narrow class group $C_+(K)$ of K. We represent general Legendre symbols

Received July 13, 2010; Revised December 13, 2010.
2010 *Mathematics Subject Classification.* 11R29, 11R45.
Key words and phrases. class group, unramified extension, quartic residue, density.
The first author was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2011-0005138).
The second author was partly supported by NNSF of China(No. 10771100, No. 10971250).

by binary quadratic forms $q^{h_+(2p)/4} = x^2 - 2py^2$ and $\pm p_2^{h_+(2p_1)/4} = 2x^2 - p_1y^2$ over $\mathbb{Z}$, where $h_+(2p_1)$ is the narrow class number of K. Meanwhile, we give some quartic reciprocity laws.

In §3, we investigate 8-ranks of class groups $C(F)$ for imaginary quadratic fields $F = \mathbb{Q}(\sqrt{\varepsilon p_1 \cdots p_{t-1}})$, where $\varepsilon \in \{-1, -2\}$ and distinct primes $p_i \equiv 1 \bmod 4$. We give the necessary and sufficient conditions for 8-ranks of $C(F)$ equal to 1 or 2 provided that 4-ranks of $C(F)$ are at most equal to 2. Their results are expressed by congruence relations of p_i modulo 2^n, general Legendre symbols and quartic residue symbols $(\frac{p_1}{p_2})_4$, $(\frac{2p_1}{p_2})_4$ (see [10]). These results are very useful for numerical calculations.

In §4, especially for $F = \mathbb{Q}(\sqrt{\varepsilon p_1 p_2})$, we compute densities for 8-ranks of $C(F)$ equal to 1 or 2 in such quadratic number fields (Theorem 4.1).

We use the following notation:

$\mathcal{O}_F$	ring of integers of a quadratic number field $F = \mathbb{Q}(\sqrt{d})$,
$C(F), C_+(F)$	ideal class group, narrow ideal class group of F,
$h(d), h_+(d)$	class number, narrow class number of $F = \mathbb{Q}(\sqrt{d})$,
$\mathfrak{p}_a$	ideal of F over an integer $a \in \mathbb{Z}$,
$[\mathfrak{p}_a]$	class of an ideal $\mathfrak{p}_a \subseteq \mathcal{O}_F$ in $C_+(F)$,
$\mathfrak{t}$	ideals of $F = \mathbb{Q}(\sqrt{d})$ over prime 2,
${}_2A$	subgroup of elements of order ≤ 2 of an abelian group A,
$r_{2^n}(A)$	2^n-rank of A,
R_F	Rédei's matrix of F,
A^+	set of primes $p \equiv 1 \bmod 8$ represented by $x^2 + 32y^2$ over $\mathbb{Z}$,
A^-	set of primes $p \equiv 1 \bmod 8$ not represented by $x^2 + 32y^2$ over $\mathbb{Z}$,
B^+	set of primes $p \equiv 1 \bmod 8$ represented by $x^2 + 64y^2$ over $\mathbb{Z}$,
B^-	set of primes $p \equiv 1 \bmod 8$ not represented by $x^2 + 64y^2$ over $\mathbb{Z}$,
$(\frac{p}{q})$, $(\frac{p}{q})_4$	Legendre symbol, quartic residue symbol.

2. Preliminaries

First, for a prime $p_1 \equiv 1 \bmod 8$, we find the cyclic extension N_+ of degree 4 over $K = \mathbb{Q}(\sqrt{2p_1})$, in which no finite prime of K ramifies. In terms of norm from $L = \mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, $p_1 = u_1^2 - 2w_1^2$ with $u_1, w_1 \in \mathbb{Z}$ and, without loss of generality, we shall always assume that

$$\pi_1 = u_1 + w_1\sqrt{2} \in L \text{ with } u_1 \equiv 1 \bmod 4,\ w_1 \equiv 0 \bmod 4,$$

which is called a *primary* element in L. In fact, w_1 is even and we can multiply $u_1 + w_1\sqrt{2}$ by the element $(1 + \sqrt{2})^2 = 3 + 2\sqrt{2}$ of norm 1, if necessary. By genus theory, 2-primary subgroup of the narrow class group $C_+(K)$ of K is a cyclic and $4|h_+(2p_1)$. Let $N_+ = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \sqrt{\pi_1})$. It is clear that N_+ is a normal extension of degree 8 over $\mathbb{Q}$. Consider the tower of relative quadratic extensions:

$$\begin{array}{c} N_+ = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \sqrt{\pi_1}) \\ | \\ K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}) \\ | \\ K = \mathbb{Q}(\sqrt{2p_1}) \\ | \\ \mathbb{Q}. \end{array}$$

Let $\mathfrak{t}$ and $\mathfrak{p}_1$ be the prime ideals of K over 2 and p_1, respectively. We can verify that $\mathfrak{t}$ and $\mathfrak{p}_1$ are unramified in N_+, so all finite primes of K are unramified in N_+ (in details, see [3]). Moreover, if $p_1 \in A^+$, then $u_1 \in \mathbb{N}$ by [1], so N_+ is the unramified cyclic extension of degree 4 over K.

Let $p_2 \equiv 1 \bmod 8$ be a prime. Then $p_2 = u_2^2 - 2w_2^2$ with $u_2, w_2 \in \mathbb{Z}$, and

$$\pi_2 = u_2 + w_2\sqrt{2} \in L \text{ with } u_2 \equiv 1 \bmod 4,\ w_2 \equiv 0 \bmod 4.$$

Suppose $(\frac{p_1}{p_2}) = 1$, so p_2 splits completely in K_1. Let $\mathfrak{p}_2' = \pi_2\mathcal{O}_L = (\pi_2)$ be a prime ideal of L over p_2 and $\mathcal{P}_2$ be a prime ideal of K_1 over $\mathfrak{p}_2'$, i.e., $\mathfrak{p}_2'|p_2$ and $\mathcal{P}_2|\mathfrak{p}_2'$. Then $\mathcal{O}_{K_1}/\mathcal{P}_2 \cong \mathcal{O}_L/\mathfrak{p}_2' \cong \mathbb{Z}/(p_2)$. Hence the general Legendre symbol ([8, p. 196])

$$\left(\frac{\pi_1}{\mathcal{P}_2}\right) = \left(\frac{\pi_1}{\mathfrak{p}_2'}\right),$$

which is denoted by $(\frac{\pi_1}{\pi_2})$. In fact,

$$\left(\frac{\pi_1}{\pi_2}\right) = 1 \Leftrightarrow x^2 \equiv \pi_1 \bmod \pi_2\mathcal{O}_L \text{ has a solution in } \mathcal{O}_L.$$

Since $\mathcal{O}_L/\mathfrak{p}_2' \cong \mathbb{Z}/(p_2)$ and $(\frac{p_1}{p_2}) = 1$, $(\frac{\pi_1}{\pi_2}) = (\frac{\bar{\pi}_1}{\pi_2})$, where $\bar{\pi}_1 = u_1 - w_1\sqrt{2}$ is the conjugate element of π_1. Hence p_2 splits completely in $L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{\pi_1})$ if and only if $(\frac{\pi_1}{\pi_2}) = 1$. By the reciprocity law ([8, Theorem 165]), we have $(\frac{\pi_1}{\pi_2}) = (\frac{\pi_2}{\pi_1})$. Therefore p_2 splits completely in N_+ if and only if $(\frac{\pi_1}{\pi_2}) = 1$. We have proved:

Lemma 2.1. *Let $p_1 \equiv p_2 \equiv 1 \bmod 8$ be primes with $(\frac{p_1}{p_2}) = 1$ and π_1, π_2 be defined as above. Then*

(i) *p_2 splits completely in N_+ if and only if $(\frac{\pi_1}{\pi_2}) = 1$.*
(ii) *p_2 splits completely in K_1 but does not in N_+ if and only if $(\frac{\pi_1}{\pi_2}) = -1$.*

In the following, we use the binary quadratic form to describe the value of $(\frac{\pi_1}{\pi_2})$. Let $H_+(K)$ be the narrow Hilbert class field of K, which is the maximal abelian extension over K in which no finite prime of K ramifies. Then $Gal(H_+(K)/K) \cong C_+(K)$ and $K \subset K_1 \subset N_+ \subset H_+(K)$. Especially, if $p_1 \in A^+$, then $N_+ \subset H(K)$, which is the Hilbert class field of K. By restriction there is an epimorphism: $C_+(K) \to Gal(N_+/K)$, where $Gal(N_+/K)$ is cyclic of order 4. Hence

$$C_+(K)/C_+(K)^4 \cong Gal(N_+/K)$$

and analogously

$$C_+(K)/C_+(K)^2 \cong Gal(K_1/K).$$

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. We have that $\mathfrak{p}$ splits completely in $N_+ \Leftrightarrow$ the Artin symbol $(\frac{N_+/K}{\mathfrak{p}}) = 1 \in Gal(N_+/K) \Leftrightarrow [\mathfrak{p}] \in C_+(K)^4$ (see [11, p. 104]). Let $\mathfrak{p}_2$ be a prime ideal of $\mathcal{O}_K$ over p_2. Then we conclude that $\mathfrak{p}_2$ splits completely in $N_+ \Leftrightarrow (\frac{\pi_1}{\pi_2}) = 1 \Leftrightarrow [\mathfrak{p}_2] \in C_+(K)^4 \Leftrightarrow [\mathfrak{p}_2]^{h_+(2p_1)/4} = 1 \Leftrightarrow p_2^{h_+(2p_1)/4} = x^2 - 2p_1y^2$ for some $x, y \in \mathbb{Z}$.

Let $\mathfrak{t}$ and $\mathfrak{p}_1$ be prime ideals of $\mathcal{O}_K$ over 2 and p_1, respectively. By genus theory, $[\mathfrak{t}], [\mathfrak{p}_1]$ and $[\mathfrak{t}\mathfrak{p}_1]$ are of order at most 2 and only one of them is the unit in $C_+(K)$. Suppose $[\mathfrak{t}]$ is of order 2. Then we have that $\mathfrak{p}_2$ splits completely in K_1 but does not in $N_+ \Leftrightarrow (\frac{\pi_1}{\pi_2}) = -1 \Leftrightarrow [\mathfrak{p}_2] \in C_+(K)^2$ and $[\mathfrak{p}_2] \notin C_+(K)^4$ $\Leftrightarrow [\mathfrak{t}][\mathfrak{p}_2]^{h_+(2p_1)/4} = 1 \in C_+(K) \Leftrightarrow p_2^{h_+(2p_1)/4} = 2x^2 - p_2y^2$ for some $x, y \in \mathbb{Z}$. Suppose $[\mathfrak{t}] = 1$ and $[\mathfrak{p}_1]$ is of order 2. Then, similarly, we have that $(\frac{\pi_1}{\pi_2}) = -1$ $\Leftrightarrow [\mathfrak{p}_1][\mathfrak{p}_2]^{h_+(2p_1)/4} = 1 \in C_+(K) \Leftrightarrow p_2^{h_+(2p_1)/4} = p_1x^2 - 2y^2$ for some $x, y \in \mathbb{Z}$. Hence we have proved:

Lemma 2.2. *Let $p_1 \equiv p_2 \equiv 1 \bmod 8$ be primes with $(\frac{p_1}{p_2}) = 1$. Then*

(i) $(\frac{\pi_1}{\pi_2}) = 1$ *if and only if* $p_2^{h_+(2p_1)/4} = x^2 - 2p_1y^2$ *for some* $x, y \in \mathbb{Z}$.
(ii) $(\frac{\pi_1}{\pi_2}) = -1$ *if and only if* $\pm p_2^{h_+(2p_1)/4} = 2x^2 - p_1y^2$ *for some* $x, y \in \mathbb{Z}$.

Moreover, for $p_2 = u_2^2 - 2w_2^2 \equiv 1 \bmod 8$, we have that $(\frac{w_2}{p_2}) = 1 = (\frac{w_2}{\pi_2})$. Since $p_2 = 2(u_2 + w_2)^2 - (u_2 + 2w_2)^2$ and $u_2 + w_2 \equiv w_2(1 - \sqrt{2}) \bmod \pi_2\mathcal{O}_L$, by [1], we conclude that

$$p_2 \in A^+ \Leftrightarrow u_2 > 0, u_2 + w_2 > 0 \Leftrightarrow \Big(\frac{u_2 + w_2}{p_2}\Big) = \Big(\frac{1 - \sqrt{2}}{\pi_2}\Big) = 1;$$

$$\Big(\frac{u_2}{p_2}\Big) = 1 \Leftrightarrow \Big(\frac{2}{p_2}\Big)_4 = 1 \Leftrightarrow p_2 \in B^+.$$

Now we describe some results about quartic reciprocity law. Let $p_1 \equiv p_2 \equiv 1 \bmod 4$ be distinct primes. Then $p_1 = a_1^2 + b_1^2, p_2 = a_2^2 + b_2^2$, $b_1 \equiv b_2 \equiv 0 \bmod 2$, over $\mathbb{Z}$ in terms of norm from $L_1 = \mathbb{Q}(i)$, where $i = \sqrt{-1}$. We shall always assume that

$$\lambda_1 = a_1 + ib_1, \lambda_2 = a_2 + ib_2 \text{ with } a_1 + b_1 \equiv a_2 + b_2 \equiv 1 \bmod 4,$$

which are called *primary* elements in L_1.

For any $\alpha \in \mathbb{Z}[i]$ with $\lambda_1 \nmid \alpha$, there exists a unique integer j $(0 \leq j \leq 3)$ such that

$$\alpha^{\frac{N(\lambda_1)-1}{4}} \equiv i^j \bmod \lambda_1\mathcal{O}_{L_1}.$$

We will define by $(\frac{\alpha}{\lambda_1})_4 = i^j$ the quartic residue symbol of α modulo λ_1. There is a fact that $(\frac{p_2}{\lambda_1})_4 = 1$ if and only if $x^4 \equiv p_2 \bmod p_1$ has a solution with $x \in \mathbb{Z}$, which is denoted by $(\frac{p_2}{p_1})_4 = 1$. There is the law of quartic reciprocity (see [10, p.123]):

$$\Big(\frac{\lambda_1}{\lambda_2}\Big)_4 = \Big(\frac{\lambda_2}{\lambda_1}\Big)_4 (-1)^{\frac{(p_1-1)(p_2-1)}{16}}.$$

Lemma 2.3. *Let $p_1 \equiv p_2 \equiv 1 \bmod 4$ be distinct primes, $p_1 = a_1^2 + b_1^2, p_2 = a_2^2 + b_2^2$, and $\lambda_1 = a_1 + ib_1, \lambda_2 = a_2 + ib_2$ be primary elements as above.*

(i) *If $(\frac{p_1}{p_2}) = 1$, then $(\frac{p_1}{p_2})_4(\frac{p_2}{p_1})_4 = (\frac{\lambda_2}{\lambda_1})$.*

(ii) *Suppose $p_1 \equiv p_2 \equiv 5 \bmod 8$ and $(\frac{p_1}{p_2}) = -1$. Then*

$$\Big(\frac{2p_1}{p_2}\Big)_4 \Big(\frac{2p_2}{p_1}\Big)_4 = i^{\frac{p_1+p_2-2}{4}} \Big(\frac{\lambda_2}{\lambda_1}\Big),$$

where we take $a_1 + b_1 \equiv a_2 + b_2 \equiv 1 \bmod 8$.

Proof. (i) Let $p_1 = \lambda_1\bar{\lambda}_1$ and $p_2 = \lambda_2\bar{\lambda}_2$, where $\bar{\lambda}_1$ and $\bar{\lambda}_2$ are the conjugate elements of λ_1 and λ_2, respectively. By the quartic reciprocity law, we have that

$$\begin{aligned}\Big(\frac{p_1}{p_2}\Big)_4\Big(\frac{p_2}{p_1}\Big)_4 = \Big(\frac{p_1}{\lambda_2}\Big)_4\Big(\frac{p_2}{\lambda_1}\Big)_4 &= \Big(\frac{\lambda_1}{\lambda_2}\Big)_4\Big(\frac{\bar{\lambda}_1}{\lambda_2}\Big)_4\Big(\frac{\lambda_2}{\lambda_1}\Big)_4\Big(\frac{\bar{\lambda}_2}{\lambda_1}\Big)_4 \\ &= \Big(\frac{\lambda_2}{\lambda_1}\Big)_4^2\Big(\frac{\lambda_2}{\bar{\lambda}_1}\Big)_4\Big(\frac{\bar{\lambda}_2}{\lambda_1}\Big)_4 = \Big(\frac{\lambda_2}{\lambda_1}\Big),\end{aligned}$$

where $(\frac{\lambda_2}{\lambda_1})_4(\frac{\bar{\lambda}_2}{\lambda_1})_4 = 1$.

(ii) Similarly, we have that

$$\begin{aligned}\Big(\frac{2p_1}{p_2}\Big)_4\Big(\frac{2p_2}{p_1}\Big)_4 &= \Big(\frac{2p_1}{\lambda_2}\Big)_4\Big(\frac{2p_2}{\lambda_1}\Big)_4 \\ &= \Big(\frac{2}{\lambda_1\lambda_2}\Big)_4\Big(\frac{p_1}{\lambda_2}\Big)_4\Big(\frac{p_2}{\lambda_1}\Big)_4 \\ &= \Big(\frac{2}{\lambda_1\lambda_2}\Big)_4\Big(\frac{\lambda_2}{\lambda_1}\Big).\end{aligned}$$

Since $p_1 \equiv 5 \bmod 8$ and $2p_1 = (a_1+b_1)^2 + (a_1-b_1)^2$, we assume that $a_1 + b_1 \equiv 1 \bmod 8$ and $a_1 - b_1 \equiv 5 \bmod 8$. Similarly, we may assume that $a_2 + b_2 \equiv 1 \bmod 8$ and $a_2 - b_2 \equiv 5 \bmod 8$. By [10, p. 136, Ex.37], we have $(\frac{1+i}{\lambda_1})_4 = i^{(a_1-b_1-b_1^2-1)/4}$. Since $2 = i^3(1+i)^2$ and $(\frac{i}{\lambda_1})_4 = i^{(p-1)/4}$, we have

$$\Big(\frac{2}{\lambda_1}\Big)_4\Big(\frac{2}{\lambda_2}\Big)_4 = i^{\frac{3(p_1-1+p_2-1)}{4}+\frac{a_1-b_1-b_1^2-1+a_2-b_2-b_2^2-1}{2}} = i^{\frac{p_1+p_2-2}{4}}.$$

In fact, since $a_1+b_1 \equiv a_2+b_2 \equiv 1 \bmod 8$, $a_1-b_1-b_1^2-1 = a_1+b_1-(b_1+1)^2 \equiv 0 \bmod 8$ and $a_2 - b_2 - b_2^2 - 1 = a_2 + b_2 - (b_2+1)^2 \equiv 0 \bmod 8$. □

3. Elements of order 8

Let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field and D be the discriminant of F. The prime discriminant is either $p^* = (-1)^{(p-1)/2}p$ if p is an odd prime or $p^* = -4, 8, -8$ if $p = 2$. Then D has the unique decomposition $D = p_1^* \cdots p_t^*$ into a product of prime discriminants and $p_t = 2$ if $2|D$. By genus theory, $r_2(C_+(F)) = t - 1$.

We will denote by $(\frac{n}{p})$ the Legendre symbol if p is an odd prime and by $(\frac{n}{2})$ the Kronecker symbol. If $(\frac{n}{p}) = (-1)^a$ with $a \in \mathbb{F}_2$, we shall write $(\frac{n}{p})' = a$. Then the Rédei matrix $R_F = (a_{ij})$ of F is the $t \times t$ matrix with $a_{ij} \in \mathbb{F}_2$ given by

$$a_{ij} = \begin{cases} (\frac{p_i^*}{p_j})' & \text{if } i \neq j, \\ (\frac{D/p_i^*}{p_i})' & \text{if } i = j, \end{cases} \quad \text{for } 1 \leq i, j \leq t.$$

Note that the sum of all rows of R_F is equal to 0. Let R'_F be the $(t-1) \times t$ matrix obtained from R_F by deleting the t-th row. Then $\operatorname{rank} R'_F = \operatorname{rank} R_F$, where the rank is always meant to the rank over $\mathbb{F}_2$.

Let $D(F)$ be the set of all positive square-free divisors q of the discriminant D. Then $D(F)$ is an elementary abelian 2-group with multiplication $q_1 \cdot q_2 = q_1q_2/(q_1, q_2)^2$, where (q_1, q_2) is the greatest common divisor of q_1, q_2. For $q \in D(F)$, we define $X_q = (x_1, \ldots, x_t)^T \in \mathbb{F}_2^t$ by

$$x_i = \begin{cases} 1 & \text{if } p_i | q, \\ 0 & \text{if } p_i \nmid q, \end{cases} \quad \text{for } 1 \leq i \leq t.$$

Then we have that $R'_F X_q = 0 \Leftrightarrow (\frac{q}{p}) = 1$ for every odd prime $p|(D/q)$ and $(\frac{-D/q}{p}) = 1$ for every odd prime $p|q \Leftrightarrow x^2 - Dy^2 = qz^2$ is solvable over $\mathbb{Z} \Leftrightarrow q \in D(F) \cap N_{F/\mathbb{Q}}(F^*)$. Hence,

$$\theta : D(F) \cap N_{F/\mathbb{Q}}(F^*) \to \{X_q : R'_F X_q = 0\}, \ q \mapsto X_q,$$

is an isomorphism. By genus theory, $\alpha : D(F) \cap N_{F/\mathbb{Q}}(F^*) \to {}_2C(F) \cap C(F)^2$ is surjective and $|\operatorname{Ker}(\alpha)| = 2$. We have the Rédei's criterion:

$$r_4(C_+(F)) = r_2(D(F) \cap N_{F/\mathbb{Q}}(F^*)) - 1 = t - 1 - \operatorname{rank} R_F.$$

We know the method of Rédei's matrix to determine the solutions of the Diophantine equations $qz^2 = x^2 - Dy^2$ over $\mathbb{Z}$. For convenience, if it has a non-trivial solution over $\mathbb{Z}$, then it will be called solvable.

Let $F = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with $d = p_1 \cdots p_{t-1}$ and distinct primes $p_i \equiv 1 \bmod 4$. Then the narrow class group $C_+(F)$ is just the class group $C(F)$ and $r_2(C(F)) = t - 1$ by genus theory. The Rédei's matrix of F is

$$(3.1)\quad R_F = \begin{pmatrix} (\frac{D/p_1^*}{p_1})' & \cdots & (\frac{p_{t-1}}{p_1})' & (\frac{p_t}{p_1})' \\ \vdots & & \vdots & \vdots \\ (\frac{p_1}{p_{t-1}})' & \cdots & (\frac{D/p_{t-1}^*}{p_{t-1}})' & (\frac{p_t}{p_{t-1}})' \\ 0 & \cdots & 0 & (\frac{p_t}{p_1\cdots p_{t-1}})' \end{pmatrix} = \begin{pmatrix} M & \alpha \\ 0 & (\frac{p_t}{p_1\cdots p_{t-1}})' \end{pmatrix},$$

where $p_t = 2$ and M is equal to the $(t-1)\times(t-1)$ Rédei's matrix R_E of the real quadratic field $E = \mathbb{Q}(\sqrt{d})$.

Proposition 3.1. *Let $F = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with $d = p_1\cdots p_{t-1}$ and distinct primes $p_i \equiv 1 \bmod 4$ $(t \geq 3)$. Let $E = \mathbb{Q}(\sqrt{d})$ be a real quadratic field. Then*

(i) *$r_4(C(F)) = 0$ if and only if $d \equiv 5 \bmod 8$ and $r_4(C_+(E)) = 0$.*
(ii) *$r_4(C(F)) = r$ $(1 \leq r \leq t-1)$ if and only if either $r_4(C_+(E)) = r-1$ and $q \equiv 1 \bmod 8$ for each $q \in D(E)$ or $r_4(C_+(E)) = r$ and there is some $q \in D(E)$ such that $q \equiv 5 \bmod 8$.*

Proof. (i) Since $p_i \equiv 1 \bmod 4$ for $1 \leq i \leq t-1$, R_E is a symmetric matrix and $\operatorname{rank} R_E \leq t-2$. By Rédei's criterion, $r_4(C(F)) = 0 \Leftrightarrow \operatorname{rank} R_F = t-1 \Leftrightarrow \operatorname{rank} R_E = t-2$ and $(\frac{2}{p_1\cdots p_{t-1}}) = -1 \Leftrightarrow r_4(C_+(E)) = 0$ and $d \equiv 5 \bmod 8$.

(ii) Suppose $r_4(C(F)) = r$, so $\operatorname{rank} R_F = t-1-r$. Note that the sum of all row vectors of R_F is equal to zero vector. We have that $\operatorname{rank} R_F = t-1-r$ if and only if either $\operatorname{rank} R_E = t-1-r$ and the vector α is linearly represented by column vectors of R_E in (3.1) or $\operatorname{rank} R_E = t-1-r-1$ and α is not linearly represented by column vectors of R_E. We only need to prove that α is linearly represented by column vectors of R_E if and only if $q \equiv 1 \bmod 8$ for each $q \in D(E)$.

If α is linearly represented by column vectors of R_E and $q = p_1\cdots p_s \in D(E)$ $(s \leq t-1)$, then $R_E X_q = 0$, where X_q is a vector corresponding with $q \in D(E)$. Hence, since R_E is a symmetric matrix, the addition with the first s columns (rows) of R_E is equal to zero vector, so $(\frac{2}{p_1\cdots p_s}) = 1$, i.e., $q = p_1\cdots p_s \equiv 1 \bmod 8$.

Conversely, since $d = p_1\cdots p_{t-1} \in D(E)$, $d \equiv 1 \bmod 8$ and $(\frac{2}{p_1\cdots p_{t-1}}) = 1$, we need prove $\operatorname{rank}(R_E, \alpha) = \operatorname{rank} R_E$. Without loss of generality, we assume that the first $k = t-1-r$ rows $\beta_1, \ldots, \beta_k$ of R_E is a maximal subset of linearly independent of all rows of R_E. If, for a row β_i $(k < i \leq t-1)$ of R_E, we have $\beta_1 + \cdots + \beta_k + \beta_i = 0$, then $q = p_1\cdots p_k p_i \in D(E)$ and $q \equiv 1 \bmod 8$. Let

$$M' = \begin{pmatrix} \beta_1 & (\frac{2}{p_1})' \\ \vdots & \vdots \\ \beta_k & (\frac{2}{p_k})' \\ \beta_i & (\frac{2}{p_i})' \end{pmatrix}.$$

Then $(\frac{2}{p_1})' + \cdots + (\frac{2}{p_k})' + (\frac{2}{p_i})' = 0$ and $\operatorname{rank} M' = k$, so the last row of M' is linearly represented by the first k rows of M'. Hence $\operatorname{rank}(R_E, \alpha) = \operatorname{rank} R_E$ and α is linearly represented by column vectors of R_E. □

Write $D^*(F) = D(F) \cap N_{F/\mathbb{Q}}(F^*)$ for simplicity.

Remark 3.2. By the process of proving Proposition 3.1, we have that

(i) $r_4(C(F)) = r_4(C_+(E))$ if and only if $D^*(F) = D^*(E)$;

(ii) $r_4(C(F)) = r_4(C_+(E)) + 1$ if and only if there is some $q | p_1 \cdots p_{t-1}$ such that $2qz^2 = x^2 + p_1 \cdots p_{t-1} y^2$ is solvable if and only if $2q \in D^*(F)$.

By Proposition 3.1, we have that $r_4(C(F)) = 1$ if and only if one of the following conditions holds:

(1) $\operatorname{rank} R_F = \operatorname{rank} R_E + 1 = t - 2$ and $D^*(F) = D^*(E) = \{1, q_1, q_2, d\}$, where at least one of $q_1 = p_1 \cdots p_r$ and $q_2 = p_{r+1} \cdots p_{t-1}$ is congruent to 5 modulo 8 $(1 \leq r < t - 1)$;

(2) $\operatorname{rank} R_F = \operatorname{rank} R_E = t - 2$ and $p_1 \cdots p_{t-1} \equiv 1 \bmod 8$, so $D^*(F) = \{1, 2q_1, 2q_2, d\}$, where $q_1 = p_1 \cdots p_r$ and $q_2 = p_{r+1} \cdots p_{t-1}$ $(0 \leq r < t-1$ and $q_1 = 1$ if $r = 0)$.

Theorem 3.3. *Let $F = \mathbb{Q}(\sqrt{-d})$, where $d = p_1 \cdots p_{t-1}$ with distinct primes $p_i \equiv 1 \bmod 4$, be an imaginary quadratic field and $r_4(C(F)) = 1$.*

(i) *Suppose $D^*(F) = \{1, q_1, q_2, d\}$, where $q_1 = p_1 \cdots p_r \equiv 1 \bmod 8$ and $q_2 = p_{r+1} \cdots p_{t-1} \equiv 5 \bmod 8$. Then $r_8(C(F)) = 1$ if and only if $(\frac{q_2}{q_1})_4 = 1$.*

(ii) *Suppose $D^*(F) = \{1, q_1, q_2, d\}$, where $q_1 = p_1 \cdots p_r \equiv 5 \bmod 8$ and $q_2 = p_{r+1} \cdots p_{t-1} \equiv 5 \bmod 8$. Then $r_8(C(F)) = 1$ if and only if $(\frac{q_1}{q_2})_4 (\frac{q_2}{q_1})_4 = -1$.*

(iii) *Suppose $D^*(F) = \{1, 2q_1, 2q_2, d\}$, where $q_1 = p_1 \cdots p_r \equiv 5 \bmod 8$ and $q_2 = p_{r+1} \cdots p_{t-1} \equiv 5 \bmod 8$. Then $r_8(C(F)) = 1$ if and only if either $d \equiv 9 \bmod 16$ and $(\frac{2q_1}{q_2})_4 (\frac{2q_2}{q_1})_4 = -1$ or either $d \equiv 1 \bmod 16$ and $(\frac{2q_1}{q_2})_4 (\frac{2q_2}{q_1})_4 = 1$.*

(iv) *Suppose $D^*(F) = \{1, 2q_1, 2q_2, d\}$, where $q_1 = p_1 \cdots p_r \equiv 1 \bmod 8$ and $q_2 = p_{r+1} \cdots p_{t-1} \equiv 1 \bmod 8$. Then $r_8(C(F)) = 1$ if and only if either $d \equiv 1 \bmod 16$ and $(\frac{2q_1}{q_2})_4 (\frac{2q_2}{q_1})_4 = -1$ or either $d \equiv 9 \bmod 16$ and $(\frac{2q_1}{q_2})_4 (\frac{2q_2}{q_1})_4 = 1$.*

Proof. (i) Suppose $\operatorname{rank} R_F = t - 2$, $D^*(F) = \{1, q_1, q_2, d\}$ and $q_1 = p_1 \cdots p_r \equiv 1 \bmod 8$, $q_2 = p_{r+1} \cdots p_{t-1} \equiv 5 \bmod 8$. Then the sum of the first r row vectors of R_F is equal to zero vector. Let $\mathfrak{q}_1^2 = q_1 \mathcal{O}_F$. Then $1 \neq [\mathfrak{q}_1] \in {}_2C(F) \cap C(F)^2$. By Rédei's criterion, $z^2 = q_1 x^2 + q_2 y^2$ has a relatively prime solution $(x, y, z) = (a, b, c)$ over $\mathbb{N}$, so $[\mathfrak{q}_1] = [\mathfrak{c}]^2 \in C(F)^2$, where $\mathfrak{c}$ is an ideal of $\mathcal{O}_F$ over c. Since $c^2 = q_1 a^2 + q_2 b^2$ and $q_1 \equiv 1 \bmod 8$, we have that the Jacobi symbols $(\frac{b}{q_1}) = 1$ and $(\frac{c}{q_1}) = (\frac{q_2}{q_1})_4$, where $(\frac{q_2}{q_1})_4 = (\frac{q_2}{p_1})_4 \cdots (\frac{q_2}{p_r})_4$. We conclude that $r_8(C(F)) = 1 \Leftrightarrow [\mathfrak{q}_1] \in C(F)^4 \Leftrightarrow [\mathfrak{c}][\mathfrak{m}] \in C(F)^2$, where $\mathfrak{m}$ is an ambiguous ideal of F over $m|2d \Leftrightarrow mcz^2 = x^2 + dy^2$ is solvable over $\mathbb{Z} \Leftrightarrow$ the following system of equations is solvable over $\mathbb{F}_2$

$$R'_F X = \begin{pmatrix} (\frac{c}{p_1})' \\ \vdots \\ (\frac{c}{p_{t-1}})' \end{pmatrix}$$

$\Leftrightarrow (\frac{c}{q_1}) = (\frac{c}{p_1 \cdots p_r}) = 1 = (\frac{c}{q_1})_4$ (since rank $R'_F = t-2$).

(ii) Suppose rank $R_F = t-2$, $D^*(F) = \{1, q_1, q_2, d\}$ and $q_1 = p_1 \cdots p_r \equiv 5 \bmod 8$, $q_2 = p_{r+1} \cdots p_{t-1} \equiv 5 \bmod 8$. Then the sum of the first $t-1$ row vectors of R_F is equal to zero and the sum of the first r row vectors of M is also equal to zero. Let $z^2 = q_1 x^2 + q_2 y^2$ have a non-trivial solution $(x,y,z) = (a,b,c)$ over $\mathbb{N}$. Then, by Rédei's criterion, $r_4(C(F)) = 1$ and $1 \neq [\mathfrak{q}_1] = [\mathfrak{c}]^2 \in {}_2C(F) \cap C(F)^2$, where $\mathfrak{q}_1^2 = q_1 \mathcal{O}_F$ and $\mathfrak{c}$ is an ideal of F over c. Since $q_1 \equiv q_2 \equiv 5 \bmod 8$, without loss of generality, $c^2 = q_1 a^2 + 4q_2 b'^2$, where $b = 2b'$ and $a \equiv b' \equiv 1 \bmod 2$. Hence the Jacobi symbol $(\frac{a}{q_2}) = 1 = (\frac{b'}{q_1}) = -(\frac{b}{q_1})$. Since $c^2 = q_1 a^2 + q_2 b^2$, we have that $(\frac{c}{q_1}) = (\frac{q_2}{q_1})_4 (\frac{b}{q_1})$ and $(\frac{c}{q_2}) = (\frac{q_1}{q_2})_4 (\frac{a}{q_2})$. Similarly, we conclude that

$$r_8(C(F)) = 1 \Leftrightarrow [\mathfrak{q}_1] \in C(F)^4 \Leftrightarrow \left(\frac{c}{q_1}\right) = \left(\frac{c}{q_2}\right) \Leftrightarrow \left(\frac{q_1}{q_2}\right)_4 \left(\frac{q_2}{q_1}\right)_4 = -1.$$

(iii) Suppose rank $R_F = t-2$ and $D^*(F) = \{1, 2q_1, 2q_2, d\}$, where $q_1 = p_1 \cdots p_r \equiv 5 \bmod 8$ and $q_2 = p_{r+1} \cdots p_{t-1} \equiv 5 \bmod 8$. Then the sum of the first $t-1$ row vectors of R_F is equal to zero vector, i.e., $(\frac{2}{p_1 \cdots p_{t-1}}) = 1$. Let $2z^2 = q_1 x^2 + q_2 y^2$ have a non-trivial solution $(x,y,z) = (a,b,c)$ over $\mathbb{N}$, where a, b, c are all odd. Then $1 \neq [\mathfrak{t}\mathfrak{q}_1] = [\mathfrak{c}]^2 \in C(F)^2$, where $\mathfrak{t}^2 = 2\mathcal{O}_F, \mathfrak{q}_1^2 = q_1 \mathcal{O}_F$, and $\mathfrak{c}$ is an ideal of F over c. Since $2c^2 = q_1 a^2 + q_2 b^2$, we have that Jacobi symbols $(\frac{2q_2}{a}) = (\frac{2q_1}{b}) = 1$ and

$$\left(\frac{c}{q_1}\right) = \left(\frac{2q_2}{q_1}\right)_4 \left(\frac{b}{q_1}\right), \quad \left(\frac{c}{q_2}\right) = \left(\frac{2q_1}{q_2}\right)_4 \left(\frac{a}{q_2}\right).$$

Since $(q_1 a)^2 + db^2 = 2q_1 c^2 \equiv 10 \bmod 16$, we have that $d \equiv 9 \bmod 16 \Leftrightarrow 9a^2 + 9b^2 \equiv 10 \bmod 16 \Leftrightarrow ab \equiv \pm 3 \bmod 8 \Leftrightarrow (\frac{2}{a}) = -(\frac{2}{b}) \Leftrightarrow (\frac{a}{q_2}) = -(\frac{b}{q_1})$; in other word, $d \equiv 1 \bmod 16 \Leftrightarrow (\frac{a}{q_2}) = (\frac{b}{q_1})$. We conclude that $r_8(C(F)) = 1$ $\Leftrightarrow [\mathfrak{t}\mathfrak{q}_1] \in C(F)^4 \Leftrightarrow (\frac{c}{d}) = 1$, i.e., $(\frac{c}{q_1}) = (\frac{c}{q_2}) \Leftrightarrow$ either $d \equiv 9 \bmod 16$ with $(\frac{2q_2}{q_1})_4 (\frac{2q_1}{q_2})_4 = -1$ or $d \equiv 1 \bmod 16$ with

$$\left(\frac{2q_2}{q_1}\right)_4 \left(\frac{2q_1}{q_2}\right)_4 = 1.$$

(iv) It is clear from the process of proving (iii). □

Let $F = \mathbb{Q}(\sqrt{-p_1 p_2})$ be an imaginary quadratic field with $p_1 \equiv p_2 \equiv 1 \bmod 4$. By Rédei's criterion, we have that $r_4(C(F)) = 1$ if and only if one of the following four conditions holds:

(1) $p_1 \equiv p_2 + 4 \equiv 1 \bmod 8$ and $(\frac{p_1}{p_2}) = 1$;
(2) $p_1 \equiv p_2 \equiv 5 \bmod 8$ and $(\frac{p_1}{p_2}) = 1$;
(3) $p_1 \equiv p_2 \equiv 5 \bmod 8$ and $(\frac{p_1}{p_2}) = -1$;
(4) $p_1 \equiv p_2 \equiv 1 \bmod 8$ and $(\frac{p_1}{p_2}) = -1$.

By Theorem 3.3 and Lemma 2.3, we have proved:

Corollary 3.4. *Let $F = \mathbb{Q}(\sqrt{-p_1p_2})$ be an imaginary quadratic field.*

(i) *Suppose $p_1 \equiv 1 \bmod 8$, $p_2 \equiv 5 \bmod 8$ and $(\frac{p_1}{p_2}) = 1$. Then $r_8(C(F)) = 1$ if and only if $(\frac{p_2}{p_1})_4 = 1$.*
(ii) *Suppose $p_1 \equiv p_2 \equiv 5 \bmod 8$ and $(\frac{p_1}{p_2}) = 1$. Then $r_8(C(F)) = 1$ if and only if $(\frac{p_2}{p_1})_4(\frac{p_1}{p_2})_4 = -1$ if and only if $(\frac{\lambda_1}{\lambda_2}) = 1$, where λ_1 and λ_2 are defined as Lemma 2.3.*
(iii) *Suppose $p_1 \equiv p_2 \equiv 5 \bmod 8$ and $(\frac{p_1}{p_2}) = -1$. Then $r_8(C(F)) = 1$ if and only if either $p_1p_2 \equiv 9 \bmod 16$ and $(\frac{2p_1}{p_2})_4(\frac{2p_2}{p_1})_4 = -1$ or $p_1p_2 \equiv 1 \bmod 16$ and $(\frac{2p_1}{p_2})_4(\frac{2p_2}{p_1})_4 = 1$ if and only if $(\frac{\lambda_1}{\lambda_2}) = 1$, where λ_1 and λ_2 are defined as Lemma 2.3.*
(iv) *Suppose $p_1 \equiv p_2 \equiv 1 \bmod 8$ and $(\frac{p_1}{p_2}) = -1$. Then $r_8(C(F)) = 1$ if and only if either $p_1, p_2 \in A^+$ or $p_1, p_2 \in A^-$ if and only if $(\frac{1-\sqrt{2}}{\pi_1\pi_2}) = 1$, where π_1 and π_2 are defined as in §2.*

Example 3.5. In Corollary 3.4, let $F = \mathbb{Q}(\sqrt{-p_1p_2})$ with distinct primes $p_1 \equiv p_2 \equiv 1 \bmod 4$. Let $C(F)_2$ denote the 2-primary subgroup of $C(F)$.

(i) For $p_1 = 17$ and $p_2 = 13$, $(\frac{17}{13}) = 1$, $3^4 = 13 + 17 \cdot 4$, $(\frac{13}{17})_4 = 1$, so $r_8(C(F)) = 1$ by Theorem 3.3(i). In fact, $C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2)$ by Pari-GP.
(ii) For $p_1 = 13$ and $p_2 = 29$, $(\frac{13}{29}) = 1$, $13 = 3^2 + 2^2$, $29 = 5^2 + 2^2$, $(\frac{13}{19})_4(\frac{29}{13})_4 = -1$ by quartic reciprocity, so $r_8(C(F)) = 1$ by Theorem 3.3(ii). In fact, $C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2)$ by Pari-GP.
(iii) For $p_1 = 13$ and $p_2 = 37$, $(\frac{37}{13}) = -1$, $p_1 \cdot p_2 \equiv 1 \bmod 16$, $2 \cdot 37 = 4^4 - 14 \cdot 13$, $2 \cdot 17 = 11^4 - 395 \cdot 37$, $(\frac{2\cdot 37}{13})_4 = (\frac{2\cdot 13}{37})_4 = 1$, so $r_8(C(F)) = 1$ by Theorem 3.3(iii). In fact, $C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2)$ by Pari-GP.
(iv) For $p_1 = 17$ and $p_2 = 73$, $p_1, p_2 \in A^-$, $r_8(C(F)) = 1$ by Theorem 3.3(iv). In fact, $C(F)_2 \cong \mathbb{Z}/(16) \oplus \mathbb{Z}/(2)$ by Pari-GP.

In Proposition 3.1, we know that $r_4(C(F)) = 2$ if and only if one of the following conditions holds:

(1) $\operatorname{rank} R_F = \operatorname{rank} R_E = t - 3$ and $D(F) = (q_1) \times (2q_1') \times (d)$, where $q_1 = p_1 \cdots p_r \equiv 1 \bmod 8$ $(1 \le r < t-1)$ and $q_1' | d$.
(2) $\operatorname{rank} R_F = \operatorname{rank} R_E + 1 = t - 3$ and $D(F) = D(E) = (q_1) \times (q_2) \times (q_3)$, where $q_1 = p_1 \cdots p_r, q_2 = p_{r+1} \cdots p_s$ and $q_3 = p_{s+1} \cdots p_{t-1}$.

Theorem 3.6. *Let $F = \mathbb{Q}(\sqrt{-d})$, where $d = p_1 \cdots p_{t-1}$ and distinct primes $p_i \equiv 1 \bmod 8$, be an imaginary quadratic field. Let $\operatorname{rank} R_F = t - 3$ and $D(F) = (q_1) \times (2) \times (d)$, where $q_1 = p_1 \cdots p_r$ $(1 \le r < t-1)$.*

(i) *Let* $\mathfrak{q}_1^2 = q_1\mathcal{O}_F$*. Then* $[\mathfrak{q}_1] \in C(F)^4$ *if and only if* $(\frac{q_1}{q_2})_4 = (\frac{q_2}{q_1})_4 = 1$*.*

(ii) *Let* $p_i = u_i^2 - 2w_i^2 \equiv 1 \bmod 8$ *and* $\pi_i = u_i + w_i\sqrt{2}$ *for* $1 \le i \le t-1$*. Let* $\pi_1' = \prod_{i=1}^r \pi_i = u_1' + w_1'\sqrt{2}$*,* $\pi_2' = \prod_{i=r+1}^{t-1} \pi_i = u_2' + w_2'\sqrt{2}$ *and* $\mathfrak{t}^2 = 2\mathcal{O}_F$*. Then* $[\mathfrak{t}] \in C(F)^4$ *if and only if* $(\frac{1-\sqrt{2}}{\pi_1'}) = (\frac{1-\sqrt{2}}{\pi_2}) = (\frac{\pi_1'}{\pi_2'})$ *if and only if either both* $p_1, \dots, p_r$ *and* $p_{r+1}, \dots, p_{t-1}$ *belonging to* A^- *are two even numbers and* $(\frac{\pi_1'}{\pi_2'}) = 1$ *or both* $p_1, \dots, p_r$ *and* $p_{r+1}, \dots, p_{t-1}$ *belonging to* A^- *are two odd numbers and* $(\frac{\pi_1'}{\pi_2'}) = -1$*. Moreover,* $r_8(C(F)) = 2$ *if and only if* $[\mathfrak{q}_1], [\mathfrak{t}] \in C(F)^4$ *if and only if* $(\frac{q_1}{q_2})_4 = (\frac{q_2}{q_1})_4 = 1$ *and* $(\frac{1-\sqrt{2}}{\pi_1'}) = (\frac{1-\sqrt{2}}{\pi_2'}) = (\frac{\pi_1}{\pi_2'})$*.*

Proof. (i) Suppose rank $R_F = t-3$ and $D(F) = (q_1) \times (2) \times (d)$, where $q_1 = p_1 \cdots p_r$ $(1 \le r < t-1)$. Then the two sums of both the first r row vectors and the first $t-1$ row vectors of R_F are equal to zero. Let $z^2 = q_1x^2 + q_2y^2$, $q_2 = d/q_1$, have a non-trivial solution $(x, y, z) = (a, b, c)$ over $\mathbb{N}$. Then $1 \ne [\mathfrak{q}_1] = [\mathfrak{c}]^2 \in C(F)^2$, where $\mathfrak{q}_1^2 = q_1\mathcal{O}_F$ and $\mathfrak{c}$ is an ideal of F over c. Since $c^2 = q_1a^2 + q_2b^2$ and $q_1 \equiv q_2 \equiv 1 \bmod 8$, the Jacobi symbols $(\frac{a}{q_2}) = (\frac{b}{q_1}) = 1$ and

$$\left(\frac{c}{q_1}\right) = \left(\frac{q_2}{q_1}\right)_4, \quad \left(\frac{c}{q_2}\right) = \left(\frac{q_1}{q_2}\right)_4.$$

We conclude that $[\mathfrak{q}_1] \in C(F)^4 \Leftrightarrow [\mathfrak{c}][\mathfrak{m}] \in C(F)^2$, where $\mathfrak{m}$ is an ambiguous ideal of F over $m|2d \Leftrightarrow mcz^2 = x^2 + dy^2$ is solvable over $\mathbb{Z} \Leftrightarrow$ the following system of equations is solvable over $\mathbb{F}_2$

$$R_F'X = \begin{pmatrix} (\frac{c}{p_1})' \\ \vdots \\ (\frac{c}{p_{t-1}})' \end{pmatrix}$$

$\Leftrightarrow (\frac{c}{q_1}) = (\frac{q_2}{q_1})_4 = 1$ and $(\frac{c}{q_2}) = (\frac{q_1}{q_2})_4 = 1$.

(ii) Since $q_1q_2 = N_{L/\mathbb{Q}}(\pi_1'\pi_2') = u^2 - 2w^2 = 2(u+w)^2 - (u+2w)^2$, where $u = u_1'u_2' + 2w_1'w_2'$ and $w = u_1'w_2' + u_2'w_1'$, we have

$$[\mathfrak{t}] = [\mathfrak{p}_{u+w}]^2 \in C(F)^2,$$

where $\mathfrak{p}_{u+w}$ is an ideal of F over $u+w$. For each p_i $(1 \le i \le r)$, $\mathcal{O}_L/(\pi_i) \cong \mathbb{Z}/(p_i)$ and $(\frac{u+w}{p_i}) = (\frac{u+w}{\pi_i})$. On the other hand,

$$\begin{aligned} u + w &= u_1'u_2' + 2w_1'w_2' + u_1'w_2' + u_2'w_1' \\ &\equiv -w_1'u_2'\sqrt{2} + 2w_1'w_2' - w_1'w_2'\sqrt{2} + u_2'w_1' \\ &\equiv w_1'(1-\sqrt{2})(u_2' - w_2'\sqrt{2}) \bmod \pi_i, \end{aligned}$$

so

$$\left(\frac{u+w}{p_i}\right) = \left(\frac{u+w}{\pi_i}\right) = \left(\frac{w_1'}{\pi_i}\right)\left(\frac{1-\sqrt{2}}{\pi_i}\right)\left(\frac{\pi_2'}{\pi_i}\right), \ 1 \le i \le r.$$

Similarly, we get:

$$\Big(\frac{u+w}{p_j}\Big)=\Big(\frac{u+w}{\pi_j}\Big)=\Big(\frac{w_2'}{\pi_j}\Big)\Big(\frac{1-\sqrt{2}}{\pi_j}\Big)\Big(\frac{\pi_1'}{\pi_j}\Big),\ r+1\le j\le t-1.$$

Since $q_1=u_1'^2-2w_1'$, $(\frac{w_1'}{q_1})=(\frac{w_1'}{\pi_1'})=1$, similarly, $(\frac{w_2'}{q_2})=(\frac{w_2'}{\pi_2'})=1$. Note the fact that $p_i\in A^+$ if and only if $(\frac{1-\sqrt{2}}{\pi_i})=1$. By reciprocity law, we know that $(\frac{\pi_1'}{\pi_2'})=(\frac{\pi_2'}{\pi_1'})$. Since $\operatorname{rank} R_F=t-2$ and $p_i\equiv 1 \bmod 8$, we conclude that $[\mathfrak{t}]\in C(F)^4 \Leftrightarrow$ the following system of equations is solvable over $\mathbb{F}_2$

$$R_F'X=\begin{pmatrix}(\frac{u+w}{p_1})'\\ \vdots\\ (\frac{u+w}{p_{t-1}})'\end{pmatrix}$$

$\Leftrightarrow$ $(\frac{u+w}{q_1})=1$ and $(\frac{u+w}{q_2})=1$ $\Leftrightarrow$ either both $p_1,\ldots,p_r$ and $p_{r+1},\ldots,p_{t-1}$ belonging to A^- are two even numbers and $(\frac{\pi_1'}{\pi_2'})=1$ or both $p_1,\ldots,p_r$ and $p_{r+1},\ldots,p_{t-1}$ belonging to A^- are two odd numbers and $(\frac{\pi_1'}{\pi_2'})=-1$. □

Let $F=\mathbb{Q}(\sqrt{-p_1p_2})$ be an imaginary quadratic field with $p_1\equiv p_2\equiv 1 \bmod 4$. By Rédei's criterion, we have that $r_4(C(F))=2$ if and only if $p_1\equiv p_2\equiv 1 \bmod 8$ and $(\frac{p_1}{p_2})=1$. By Theorem 3.6 and Lemma 2.2, we have proved:

Corollary 3.7. *Let $F=\mathbb{Q}(\sqrt{-p_1p_2})$ be an imaginary quadratic field with primes $p_1\equiv p_2\equiv 1 \bmod 8$ and $(\frac{p_1}{p_2})=1$. Let $\mathfrak{p}_1^2=p_1\mathcal{O}_F$ and $\mathfrak{t}^2=2\mathcal{O}_F$. Then*

(i) $[\mathfrak{p}_1]\in C(F)^4$ *if and only if* $(\frac{p_1}{p_2})_4=(\frac{p_2}{p_1})_4=1$.

(ii) $[\mathfrak{t}]\in C(F)^4$ *if and only if* $(\frac{\pi_1}{\pi_2})=(\frac{1-\sqrt{2}}{\pi_1})=(\frac{1-\sqrt{2}}{\pi_2})$ *if and only if either* $p_1,p_2\in A^+$ *and* $(\frac{\pi_1}{\pi_2})=1$, *or* $p_1,p_2\in A^-$ *and* $(\frac{\pi_1}{\pi_2})=-1$ *if and only if either* $p_1,p_2\in A^+$ *and* $p_2^{h_+(2p_1)/4}=x^2-2p_1y^2$ *for some* $x,y\in\mathbb{Z}$, *or* $p_1,p_2\in A^-$ *and* $\pm p_2^{h_+(2p_1)/4}=2x^2-p_1y^2$ *for some* $x,y\in\mathbb{Z}$, *where* π_1 *and* π_2 *are defined as in* §2. *Moreover,* $r_8(C(F))=2$ *if and only if* $[\mathfrak{p}_1],[\mathfrak{t}]\in C(F)^4$ *if and only if* $(\frac{p_1}{p_2})_4=(\frac{p_2}{p_1})_4=1$ *and* $(\frac{\pi_1}{\pi_2})=(\frac{1-\sqrt{2}}{\pi_1})=(\frac{1-\sqrt{2}}{\pi_2})$.

We now turn to another imaginary quadratic fields $F=\mathbb{Q}(\sqrt{-2d})$ with $d=p_1\cdots p_{t-1}$ and distinct primes $p_i\equiv 1 \bmod 4$. We know that $r_2(C(F))=t-1$ by genus theory and the Rédei's matrix R_F is a symmetric matrix. We have that $r_4(C(F))=1$ if and only if $\operatorname{rank} R_F=t-2$ and $D^*(F)=\{1,q_1,2q_2,2d\}$, where $q_1=p_1\cdots p_r$ and $q_2=p_{r+1}\cdots p_{t-1}$.

Theorem 3.8. *Let $F=\mathbb{Q}(\sqrt{-2d})$ be an imaginary quadratic field with $d=p_1\cdots p_{t-1}$ and distinct primes $p_i\equiv 1 \bmod 4$. Let* $\operatorname{rank} R_F=t-2$ *and* $D^*(F)=\{1,q_1,2q_2,2d\}$.

(i) *Suppose* $q_1 = p_1 \cdots p_r \equiv 1 \bmod 8$, $q_2 = p_{r+1} \cdots p_{t-1}$ *and* $1 \le r < t-1$. *Then* $r_8(C(F)) = 1$ *if and only if* $(\frac{2q_2}{q_1})_4 = 1$.

(ii) *Suppose* $p_i \equiv 1 \bmod 8$ *for* $1 \le i \le t-1$, *that is,* $q_1 = d$ *and* $q_2 = 1$. *Then* $r_8(C(F)) = 1$ *if and only if an even number of the primes* $p_1, \ldots, p_{t-1}$ *belong to* B^-.

Proof. (i) Suppose rank $R_F = t-2$ and $q_1 = p_1 \cdots p_r \in D(F)$. Then the sum of the first r row vectors of R_F is equal to zero. Let $z^2 = q_1x^2 + 2q_2y^2$ have a relatively prime solution $(x, y, z) = (a, b, c)$ over $\mathbb{N}$. Then $[\mathfrak{q}_1] = [\mathfrak{p}_c]^2 \in C(F)^2$, where $\mathfrak{q}_1^2 = q_1\mathcal{O}_F$ and $\mathfrak{p}_c$ is an ideal of F over c. Since $c^2 = q_1a^2 + 2q_2b^2$ and $q_1 \equiv 1 \bmod 8$, we have that $(\frac{b}{q_1}) = 1$ and $(\frac{c}{q_1}) = (\frac{2q_2}{q_1})_4$. Similarly, we conclude that

$$r_8(C(F)) = 1 \Leftrightarrow [\mathfrak{q}_1] \in C(F)^4 \Leftrightarrow \left(\frac{c}{q_1}\right) = \left(\frac{2q_2}{q_1}\right)_4 = 1.$$

(ii) Let $\mathfrak{t}^2 = 2\mathcal{O}_F$. Then by the process of proving (i), we conclude that $r_8(C(F)) = 1 \Leftrightarrow [\mathfrak{t}] \in C(F)^4 \Leftrightarrow (\frac{2}{p_1 \cdots p_{t-1}})_4 = 1 \Leftrightarrow$ an even number of the primes $p_1, \ldots, p_{t-1}$ belong to B^-. □

Let $F = \mathbb{Q}(\sqrt{-2p_1p_2})$ be an imaginary quadratic field with $p_1 \equiv p_2 \equiv 1 \bmod 4$. By Rédei's criterion, we have that $r_4(C(F)) = 1$ if and only if one of the following conditions holds:

(1) $p_1 \equiv p_2 + 4 \equiv 1 \bmod 8$ and $(\frac{p_1}{p_2}) = 1$;

(2) $p_1 \equiv p_2 \equiv 1 \bmod 8$ and $(\frac{p_1}{p_2}) = -1$.

By Theorem 3.8, we get:

Corollary 3.9. *Let* $F = \mathbb{Q}(\sqrt{-2p_1p_2})$ *be an imaginary quadratic field.*

(i) *Suppose* $p_1 \equiv p_2 + 4 \equiv 1 \bmod 8$ *and* $(\frac{p_1}{p_2}) = 1$. *Then* $r_8(C(F)) = 1$ *if and only if* $(\frac{2p_2}{p_1})_4 = 1$.

(ii) *Suppose* $p_1 \equiv p_2 \equiv 1 \bmod 8$ *and* $(\frac{p_1}{p_2}) = -1$. *Then* $r_8(C(F)) = 1$ *if and only if* $(\frac{2}{p_1p_2})_4 = 1$ *if and only if either* $p_1, p_2 \in B^+$ *or* $p_1, p_2 \in B^-$.

Example 3.10. In Corollary 3.9, let $F = \mathbb{Q}(\sqrt{-2p_1p_2})$ with distinct primes $p_1 \equiv p_2 \equiv 1 \bmod 4$. Let $C(F)_2$ denote the 2-primary subgroup of $C(F)$.

(i) For $p_1 = 17$ and $p_2 = 53$, $(\frac{53}{17}) = (\frac{2}{17}) = 1$, $(\frac{2p_2}{p_1})_4 = (\frac{2 \cdot 53}{17})_4 = (\frac{4}{17})_4 = 1$, so $r_8(C(F)) = 1$ by Corollary 3.9(i). In fact, $C(F)_2 \cong \mathbb{Z}/(16) \oplus \mathbb{Z}/(2)$ by Pari-GP.

(ii) For $p_1 = 17$ and $p_2 = 97$, $(\frac{97}{17}) = (\frac{12}{17}) = -1$ and $17, 97 \in B^-$, so $r_8(C(F)) = 1$ by Corollary 3.9(ii). In fact, $C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2)$ by Pari-GP.

Let $F = \mathbb{Q}(\sqrt{-2d})$ be an imaginary quadratic field with $d = p_1 \cdots p_{t-1}$ and distinct primes $p_i \equiv 1 \bmod 8$. Then the Rédei's matrix is

$$R_F = \begin{pmatrix} M & 0 \\ 0 & 0 \end{pmatrix},$$

where the $(t-1)\times(t-1)$ matrix M is equal to the Rédei's matrix R_E of $E=\mathbb{Q}(\sqrt{d})$. Let $p_i=u_i^2-2w_i^2$ and $\pi_i=u_i+w_i\sqrt{2}$ for $1\le i\le t-1$.

Theorem 3.11. *Let $F=\mathbb{Q}(\sqrt{-2d})$ be an imaginary quadratic field with $d=p_1\cdots p_{t-1}$ and distinct primes $p_i\equiv 1 \bmod 8$. Suppose* rank $R_F=t-3$, *that is, $D(F)=(2)\times(q_1)\times(2d)$, where $q_1=p_1\cdots p_r$ and $q_2=p_{r+1}\cdots p_{t-1}$. Let $\mathfrak{q}_1^2=q_1\mathcal{O}_F, \mathfrak{t}^2=2\mathcal{O}_F$, $\pi_1'=\prod_{i=1}^r\pi_i=u_1'+w_1'\sqrt{2}$ and $\pi_2'=\prod_{i=r+1}^{t-1}\pi_i=u_2'+w_2'\sqrt{2}$. Then we have*

(i) *$[\mathfrak{t}]\in C(F)^4$ if and only if $(\frac{2}{q_1})_4=(\frac{2}{q_2})_4=(\frac{\pi_2'}{\pi_1'})$ if and only if either both $p_1,\dots,p_r$ and $p_{r+1},\dots,p_{t-1}$ belonging to B^- are two even numbers and $(\frac{\pi_1'}{\pi_2'})=1$ or both $p_1,\dots,p_r$ and $p_{r+1},\dots,p_{t-1}$ belonging to B^- are two odd numbers and $(\frac{\pi_1'}{\pi_2'})=-1$.*

(ii) *$[\mathfrak{q}_1]\in C(F)^4$ if and only if $(\frac{2q_2}{q_1})_4=(\frac{q_1}{q_2})_4(\frac{\pi_1'}{\pi_2'})=1$.*

Proof. (i) By the assumption, we know that the two sums of both the first r row vectors and the first $t-1$ row vectors of R_F are equal to zero. Since $d=q_1q_2=u^2-2w^2$, where $u=u_1'u_2'+2w_1'w_2'$ and $w=u_1'w_2'+u_2'w_1'$, $2u^2=4w^2+2d$ and $[\mathfrak{t}]=[\mathfrak{p}_u]^2\in C(F)^2$, where $\mathfrak{p}_u$ is an ideal of F over u. Similarly, we conclude that

$$[\mathfrak{t}]\in C(F)^4 \Leftrightarrow \left(\frac{u}{q_1}\right)=\left(\frac{u}{q_2}\right)=1.$$

On the other hand, for each p_i $(1\le i\le r)$, $\mathcal{O}_L/(\pi_i)\cong\mathbb{Z}/(p_i)$, $u=u_1'u_2'+2w_1'w_2'\equiv u_1'(u_2'-w_2'\sqrt{2}) \bmod (\pi_i)$ and $(\frac{\pi_2'}{\pi_i})=(\frac{u_2'-w_2'\sqrt{2}}{\pi_i})$ since $(\frac{q_2}{p_i})=(\frac{q_2}{\pi_i})=1$. Then

$$\left(\frac{u}{p_i}\right)=\left(\frac{u}{\pi_i}\right)=\left(\frac{u_1'}{\pi_i}\right)\left(\frac{\pi_2'}{\pi_i}\right)=\left(\frac{u_1'}{p_i}\right)\left(\frac{\pi_2'}{\pi_i}\right).$$

Similarly, for each p_j $(r+1\le j\le t-1)$,

$$\left(\frac{u}{p_j}\right)=\left(\frac{u}{\pi_j}\right)=\left(\frac{u_2'}{\pi_j}\right)\left(\frac{\pi_1'}{\pi_j}\right)=\left(\frac{u_2'}{p_j}\right)\left(\frac{\pi_1'}{\pi_j}\right).$$

Since $q_1=u_1'^2-2w_1'^2$, we have that $(\frac{w_1'}{q_1})=1$ and $(\frac{2}{q_1})_4=(\frac{u_1'}{q_1})$, similarly, $(\frac{2}{q_2})_4=(\frac{u_2'}{q_2})$. By reciprocity law, $(\frac{\pi_1'}{\pi_2'})=(\frac{\pi_2'}{\pi_1'})$. Hence we conclude that $[\mathfrak{t}]\in C(F)^4\Leftrightarrow(\frac{2}{q_1})_4=(\frac{2}{q_2})_4=(\frac{\pi_2'}{\pi_1'})\Leftrightarrow$ either both $p_1,\dots,p_r$ and $p_{r+1},\dots,p_{t-1}$ belonging to B^- are two even numbers and $(\frac{\pi_1'}{\pi_2'})=1$ or both $p_1,\dots,p_r$ and $p_{r+1},\dots,p_{t-1}$ belonging to B^- are two odd numbers and $(\frac{\pi_1'}{\pi_2'})=-1$.

(ii) Let $z^2=q_1x^2+2q_2y^2$, where $q_1=p_1\cdots p_r$ and $q_2=d/q_1$, have a relatively prime solution $(x,y,z)=(a,b,c)$ over $\mathbb{N}$. Then $[\mathfrak{q}_1]=[\mathfrak{p}_c]^2\in C(F)^2$, where $\mathfrak{q}_1^2=q_1\mathcal{O}_F$ and $\mathfrak{p}_c$ is an ideal of F over c. Since $c^2=q_1a^2+2q_2b^2$, we have that $(\frac{b}{q_1}) = 1$ and $(\frac{c}{q_1}) = (\frac{2q_2}{q_1})_4$, $(\frac{c}{q_2}) = (\frac{q_1}{q_2})_4(\frac{a}{q_2})$. Similarly, we have that

$$[\mathfrak{q}_1] \in C(F)^4 \Leftrightarrow \Big(\frac{c}{q_1}\Big) = \Big(\frac{c}{q_2}\Big) = 1.$$

We need to determine the value of the Jacobi symbol $(\frac{a}{q_1})$. Let $2u^2 = 4w^2 + 2d$ and $q_1c^2 = (q_1a)^2 + 2db^2$. Then $2q_1u^2c^2 = N_{F/\mathbb{Q}}(q_1a + b\sqrt{-2d})N_{F/\mathbb{Q}}(2w + \sqrt{-2d})$, i.e.,

$$2q_1u^2c^2 = 4q_1^2(aw - q_2b)^2 + 2d(q_1a + 2bw)^2. \tag{3.2}$$

We can choose a solution $(x, y, z) = (a, b, c)$ of the equation $z^2 = q_1x^2 + 2q_2y^2$ such that the greatest common divisor $(uc, aw - q_2b) = 1$. In fact, in $F = \mathbb{Q}(\sqrt{-2d})$, let $\mathfrak{t}\mathfrak{p}_u^2 = (2w+\sqrt{-2d})\mathcal{O}_F$, where $\mathfrak{t}$ is the dyadic ideal of F and $\mathfrak{p}_u$ is an ideal of F over u. Since $[\mathfrak{q}_1] \in C(F)^2$, there is an ideal $\mathfrak{p}_c$ of F over positive integer number c such that $[\mathfrak{q}_1][\mathfrak{p}_c]^2 = 1$ and $\mathfrak{p}_c + \bar{\mathfrak{p}}_c = \mathcal{O}_F = \mathfrak{p}_u + \bar{\mathfrak{p}}_c$, where $\bar{\mathfrak{p}}_c$ is the conjugate ideal of $\mathfrak{p}_c$. Hence $\mathfrak{q}_1\mathfrak{p}_c^2 = (a + b\sqrt{-2d})\mathcal{O}_F$ and we get such $(x, y, z) = (a, b, c)$ satisfying $(uc, aw - q_2b) = 1$.

By (3.2), we have the Jacobi symbol $(\frac{aw-q_2b}{q_2}) = (\frac{aw}{q_2}) = 1$, i.e., $(\frac{a}{q_2}) = (\frac{w}{q_2})$. On the other hand,

$$\begin{aligned} q_1q_2 &= N_{L/\mathbb{Q}}(u_1' + w_1\sqrt{2})N_{L/\mathbb{Q}}(u_2' + w_2'\sqrt{2}) \\ &= (u_1'u_2' + 2w_1'w_2')^2 - 2(u_1'w_2' + u_2'w_1')^2 = u^2 - 2w^2, \end{aligned}$$

where $u = u_1'u_2' + 2w_1'w_2'$ and $w = u_1'w_2' + u_2'w_1'$. For each p_j $(r+1 \le j \le t-1)$, $\mathcal{O}_L/(\pi_j) \cong \mathbb{Z}/(p_j)$, $w = u_1'w_2 + u_2'w_1' \equiv w_2'(u_1' - w_1\sqrt{2}) \bmod (\pi_j)$. Hence

$$\Big(\frac{w}{p_j}\Big) = \Big(\frac{w}{\pi_j}\Big) = \Big(\frac{w_2'}{\pi_j}\Big)\Big(\frac{u_1' - w_1'\sqrt{2}}{\pi_j}\Big) = \Big(\frac{w_2'}{p_j}\Big)\Big(\frac{u_1' - w_1'\sqrt{2}}{\pi_j}\Big).$$

Since $q_2 = u_2'^2 - 2w_2'^2$, the Jacobi symbol $(\frac{w_2'}{q_2}) = 1$; by $(\frac{q_1}{q_2}) = 1$, $(\frac{\pi_1'}{\pi_2'}) = (\frac{u_1'-w_1'\sqrt{2}}{\pi_2'})$. Hence $(\frac{a}{q_2}) = (\frac{w}{q_2}) = (\frac{\pi_1'}{\pi_2})$. As a conclusion, we get that

$$[\mathfrak{q}_1] \in C(F)^4 \Leftrightarrow \Big(\frac{2q_2}{q_1}\Big)_4 = \Big(\frac{q_1}{q_2}\Big)_4\Big(\frac{\pi_1'}{\pi_2'}\Big) = 1.$$

□

Let $F = \mathbb{Q}(\sqrt{-2p_1p_2})$ be an imaginary quadratic field with distinct primes $p_1 \equiv p_2 \equiv 1 \bmod 4$. By Rédei's criterion, we have that $r_4(C(F)) = 2$ if and only if $p_1 \equiv p_2 \equiv 1 \bmod 8$ and $(\frac{p_1}{p_2}) = 1$. By Theorem 3.11 and Lemma 2.2, we get:

Corollary 3.12. *Let $F = \mathbb{Q}(\sqrt{-2p_1p_2})$ be an imaginary quadratic field with district primes $p_1 \equiv p_2 \equiv 1 \bmod 8$ and $(\frac{p_1}{p_2}) = 1$. Let $\mathfrak{t}^2 = 2\mathcal{O}_F$ and $\mathfrak{p}_1^2 = p_1\mathcal{O}_F$. Then*

(i) *$[\mathfrak{t}] \in C(F)^4$ if and only if $(\frac{2}{p_1})_4 = (\frac{2}{p_2})_4 = (\frac{\pi_1}{\pi_2})$ if and only if either $p_1, p_2 \in B^+, p_2^{h_+(2p_1)/4} = x^2 - 2p_1y^2$ over $\mathbb{Z}$ or $p_1, p_2 \in B^-, \pm p_2^{h_+(2p_1)/4} = 2x^2 - p_1y^2$ over $\mathbb{Z}$.*

(ii) $[\mathfrak{p}_1] \in C(F)^4$ *if and only if* $(\frac{2p_2}{p_1})_4 = (\frac{p_1}{p_2})_4 \cdot (\frac{\pi_1}{\pi_2}) = 1$. *Moreover,* $r_8(C(F)) = 2$ *if and only if* $(\frac{p}{q})_4 = (\frac{q}{p})_4 = (\frac{2}{p})_4 = (\frac{2}{q})_4 = (\frac{\pi_1}{\pi_2})$.

Example 3.13. Let $F = \mathbb{Q}(\sqrt{-2 \cdot 41 \cdot 241})$, $(\frac{241}{41}) = 1$. Then $C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(8)$ by Pari-GP. We also verify the condition of Corollary 3.12. It is clear that $41 = 3^2 + 32, 41 \in A^+, 41, 241 \in B^-$ and $(\frac{241}{41})_4 = (\frac{36}{41})_4 = (\frac{2}{41})(\frac{3}{41}) = -1$. In terms of norm from $\mathbb{Q}(\sqrt{-1})$, $41 = 5^2 + 4^2$, $241 = 15^2 + 4^2$, $(\frac{41}{241})_4(\frac{241}{41})_4 = (-1)^{\frac{41-1}{4}}(\frac{15 \cdot 4 - 15 \cdot 4}{41}) = 1$ by quartic reciprocity. So $(\frac{41}{241})_4 = -1$. By $41 = 13^2 - 2 \cdot 8^2$, $241 = 29^2 - 2 \cdot 20^2$, let $\pi_1 = 13 - 8\sqrt{2}$ and $\pi_2 = 29 - 20\sqrt{2}$. Then $(\frac{\pi_2}{\pi_1}) = (\frac{29 \cdot 2 - 40\sqrt{2}}{13 - 8\sqrt{2}})(\frac{2}{13 - 8\sqrt{2}}) = (\frac{-7 \cdot 2}{41}) = -1$. Hence, the 8-rank of $C(F)$ is equal to 2 by Corollary 3.12.

4. Densities

In the section, we use a Gerth's method (see [4, 5, 6, 16]) to investigate the densities of 8-rank of $C(F)$ equal to 1 or 2 in all quadratic number fields $F = \mathbb{Q}(\sqrt{-\varepsilon p_1 p_2})$, where $\varepsilon \in \{1, 2\}$ and $p_1 \equiv p_2 \equiv 1 \bmod 4$. For a positive real number x, let

$$\begin{aligned} A_x &= \{p_1 p_2 : \text{ distinct primes } p_1 \equiv p_2 \equiv 1 \bmod 4, p_1 < p_2 \text{ and } p_1 p_2 \le x\}, \\ A_{1,x} &= \{F = \mathbb{Q}(\sqrt{-p_1 p_2}) : r_4(C(F)) = r_8(C(F)) = 1 \text{ and } p_1 p_2 \in A_x\}, \\ A_{2,x} &= \{F = \mathbb{Q}(\sqrt{-p_1 p_2}) : r_4(C(F)) = r_8(C(F)) = 2 \text{ and } p_1 p_2 \in A_x\}, \\ A_{3,x} &= \{F = \mathbb{Q}(\sqrt{-2 p_1 p_2}) : r_4(C(F)) = r_8(C(F)) = 1 \text{ and } p_1 p_2 \in A_x\}, \\ A_{4,x} &= \{F = \mathbb{Q}(\sqrt{-2 p_1 p_2}) : r_4(C(F)) = r_8(C(F)) = 2 \text{ and } p_1 p_2 \in A_x\}. \end{aligned}$$

We define densities d_i $(1 \le i \le 4)$ as follows:

$$d_i = \lim_{x \to \infty} \frac{|A_{i,x}|}{|A_x|}. \tag{4.1}$$

Theorem 4.1. *Let* d_1, d_2, d_3 *and* d_4 *be defined as* (4.1). *Then*

$$d_1 = \frac{5}{16},\ d_2 = \frac{1}{128},\ d_3 = \frac{3}{16},\ d_4 = \frac{1}{128}.$$

Proof. We know that, by ([7, Theorem 437]) and $p_1 \equiv p_2 \equiv 1 \bmod 4$, $p_1 < p_2$,

$$|A_x| = \sum_{p_1 p_2 \in A_x} 1 = \frac{x \log \log x}{4 \log x} + o\Big(\frac{x \log \log x}{\log x}\Big).$$

Let $F = \mathbb{Q}(\sqrt{-p_1 p_2}) \in A_{1,x}$. Then by Corollary 3.4, we have that $r_4(C(F)) = r_8(C(F)) = 1$ if and only if one of the following five conditions holds:

(1) $p_1 \equiv p_2 + 4 \equiv 1 \bmod 8$, $(\frac{p_2}{p_1}) = 1$ and $(\frac{p_2}{p_1})_4 = 1$;
(2) $p_1 + 4 \equiv p_2 \equiv 1 \bmod 8$, $(\frac{p_2}{p_1}) = 1$ and $(\frac{p_1}{p_2})_4 = 1$;
(3) $p_1 \equiv p_2 \equiv 5 \bmod 8$, $(\frac{p_2}{p_1}) = 1$ and $(\frac{\lambda_2}{\lambda_1}) = 1$, where λ_1, λ_2 are defined as Lemma 2.3;

(4) $p_1 \equiv p_2 \equiv 5 \bmod 8$, $(\frac{p_2}{p_1}) = -1$ and $(\frac{\lambda_2}{\lambda_1}) = 1$, where λ_1, λ_2 are defined as Lemma 2.3;

(5) $p_1 \equiv p_2 \equiv 1 \bmod 8$, $(\frac{p_2}{p_1}) = -1$ and $(\frac{1-\sqrt{2}}{\pi_1\pi_2}) = 1$, where π_1, π_2 are defined as §2.

Hence

$$\begin{aligned} |A_{1,x}(F)| &= \sum_{\substack{p_1p_2\in A_x \\ p_1\equiv p_2+4\equiv 1 \bmod 8}} \frac{1}{4}\Big(1+\Big(\frac{p_2}{p_1}\Big)\Big)\Big(1+\Big(\frac{p_2}{p_1}\Big)_4\Big) \\ &+ \sum_{\substack{p_1p_2\in A_x \\ p_1+4\equiv p_2\equiv 1 \bmod 8}} \frac{1}{4}\Big(1+\Big(\frac{p_2}{p_1}\Big)\Big)\Big(1+\Big(\frac{p_1}{p_2}\Big)_4\Big) \\ &+ \sum_{\substack{p_1p_2\in A_x \\ p_1\equiv p_2\equiv 5 \bmod 8}} \frac{1}{4}\Big(1+\Big(\frac{p_2}{p_1}\Big)\Big)\Big(1+\Big(\frac{\lambda_2}{\lambda_1}\Big)\Big) \\ &+ \sum_{\substack{p_1p_2\in A_x \\ p_1\equiv p_2\equiv 5 \bmod 8}} \frac{1}{4}\Big(1-\Big(\frac{p_2}{p_1}\Big)\Big)\Big(1+\Big(\frac{\lambda_2}{\lambda_1}\Big)\Big) \\ &+ \sum_{\substack{p_1p_2\in A_x \\ p_1\equiv p_2\equiv 1 \bmod 8}} \frac{1}{4}\Big(1-\Big(\frac{p_2}{p_1}\Big)\Big)\Big(1+\Big(\frac{1-\sqrt{2}}{\pi_1\pi_2}\Big)\Big) \\ &= \sum_{pq\in A_x} \Big(\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}\Big) + o\Big(\frac{x\log\log x}{\log x}\Big) \\ &= \frac{5}{64}\cdot\frac{x\log\log x}{\log x} + o\Big(\frac{x\log\log x}{\log x}\Big). \end{aligned}$$

An intuitive explanation of the formula might proceed as follows. In the second equation, a factor of $\frac{1}{4}$ is introduced by each congruence relation of $p_1, p_2 \bmod 8$. This is considered in detail in [4, 6].

For the sake of completeness, we give a sketch of proof.

$$\begin{aligned} &\sum_{\substack{p_1p_2\in A_x \\ p_1\equiv p_2+4\equiv 1 \bmod 8}} \frac{1}{4}\Big(1+\Big(\frac{p_2}{p_1}\Big)\Big)\Big(1+\Big(\frac{p_2}{p_1}\Big)_4\Big) \\ &= \frac{1}{16}\sum_{p_1p_2\in A_x} 1 + O\left(\sum_{\substack{p_1p_2\in A_x \\ p_1\equiv p_2+4\equiv 1 \bmod 8}} \Big(\chi_1(p_2)+\chi_2(p_2)+\chi_3(p_2)\Big)\right) \\ &= \frac{x\log\log x}{64\log x} + o\Big(\frac{x\log\log x}{\log x}\Big), \end{aligned}$$

where $\chi_1(p_2) = (\frac{p_2}{p_1})$, $\chi_2(p_2) = (\frac{p_2}{p_1})_4$, $\chi_3(p_3) = (\frac{p_2}{p_1})_4(\frac{p_2}{p_1})$ are Dirichlet characters modulo p_1. By [6, Theorem 2], we have that

$$\sum \chi_i(p_2) = o\Big(\frac{x\log\log x}{\log x}\Big) \quad \text{for } i = 1, 2, 3.$$

Similarly, we have above character sum estimate for the product of characters: $(\frac{p_2}{p_1})$, $(\frac{p_2}{p_1})_4$, $(\frac{\lambda_2}{\lambda_1})$, $(\frac{1-\sqrt{2}}{\pi_1\pi_2})$.

Hence

$$d_1 = \lim_{x\to\infty} \frac{|A_{1,x}|}{|A_x|} = \frac{5}{16}.$$

Let $F = \mathbb{Q}(\sqrt{-p_1p_2}) \in A_{2,x}$. Then, by Corollary 3.7, we have that $r_4(C(F)) = r_8(C(F)) = 2$ if and only if $p_1 \equiv p_2 \equiv 1 \bmod 8$, $(\frac{p_1}{p_2})_4 = (\frac{p_2}{p_1})_4 = 1$ and $(\frac{\pi_1}{\pi_2}) = (\frac{1-\sqrt{2}}{\pi_1}) = (\frac{1-\sqrt{2}}{\pi_2})$. Hence

$$\begin{aligned} |A_{2,x}(F)| &= \sum_{\substack{p_1p_2\in A_x\\ p_1\equiv p_2\equiv 1 \bmod 8}} \frac{1}{32}\Big(1+\Big(\frac{p_2}{p_1}\Big)\Big)\Big(1+\Big(\frac{p_2}{p_1}\Big)_4\Big)\Big(1+\Big(\frac{p_1}{p_2}\Big)_4\Big) \\ &\qquad \times\Big(1+\Big(\frac{\pi_1(1-\sqrt{2})}{\pi_2}\Big)\Big)\Big(1+\Big(\frac{1-\sqrt{2}}{\pi_1\pi_2}\Big)\Big) \\ &= \sum_{\substack{p_1p_2\in A_x\\ p_1\equiv p_2\equiv 1 \bmod 8}} \frac{1}{32} + o\Big(\frac{x\log\log x}{\log x}\Big) \\ &= \frac{x\log\log x}{512\log x} + o\Big(\frac{x\log\log x}{\log x}\Big). \end{aligned}$$

Thus

$$d_2 = \lim_{x\to\infty} \frac{|A_{2,x}|}{|A_x|} = \frac{1}{128}.$$

Let $F = \mathbb{Q}(\sqrt{-2p_1p_2}) \in A_{3,x}$. Then, by Corollary 3.9, we have that $r_4(C(F)) = r_8(C(F)) = 1$ if and only if one of the following three conditions holds:

(1) $p_1 \equiv p_2 + 4 \equiv 1 \bmod 8$, $(\frac{p_1}{p_2}) = 1$ and $(\frac{2p_2}{p_1})_4 = 1$;
(2) $p_2 \equiv p_1 + 4 \equiv 1 \bmod 8$, $(\frac{p_1}{p_2}) = 1$ and $(\frac{2p_1}{p_2})_4 = 1$;
(3) $p_1 \equiv p_2 \equiv 1 \bmod 8$, $(\frac{p_1}{p_2}) = -1$ and $(\frac{2}{p_1p_2})_4 = 1$.

Hence

$$\begin{aligned} |A_{3,x}| &= \sum_{\substack{p_1p_2\in A_x\\ p_1\equiv p_2+4\equiv 1 \bmod 8}} \frac{1}{4}\Big(1+\Big(\frac{p_2}{p_1}\Big)\Big)\Big(1+\Big(\frac{2p_2}{p_1}\Big)_4\Big) \\ &\quad + \sum_{\substack{p_1p_2\in A_x\\ p_2\equiv p_1+4\equiv 1 \bmod 8}} \frac{1}{4}\Big(1+\Big(\frac{p_1}{p_2}\Big)\Big)\Big(1+\Big(\frac{2p_1}{p_2}\Big)_4\Big) \\ &\quad + \sum_{\substack{p_1p_2\in A_x\\ p_1\equiv p_2\equiv 1 \bmod 8}} \frac{1}{4}\Big(1-\Big(\frac{p_1}{p_2}\Big)\Big)\Big(1+\Big(\frac{2}{p_1p_2}\Big)_4\Big) \\ &= \sum_{p_1p_2\in A_x} \Big(\frac{1}{16}+\frac{1}{16}+\frac{1}{16}\Big) + o\Big(\frac{x\log\log x}{\log x}\Big) \end{aligned}$$

$$= \quad \frac{3}{64} \cdot \frac{x \log\log x}{\log x} + o\Big(\frac{x \log\log x}{\log x}\Big).$$

Hence

$$d_3 = \lim_{x\to\infty} \frac{|A_{3,x}|}{|A_x|} = \frac{3}{16}.$$

Let $F = \mathbb{Q}(\sqrt{-2p_1p_2}) \in A_{4,x}$. Then by Corollary 3.12, we have that $r_4(C(F)) = r_8(C(F)) = 2$ if and only if $p_1 \equiv p_2 \equiv 1 \bmod 8$, $(\frac{p_1}{p_2})_4 = (\frac{p_2}{p_1})_4 = (\frac{2}{p_1})_4 = (\frac{2}{p_2})_4 = (\frac{\pi_1}{\pi_2})$. Hence

$$\begin{aligned} |A_{4,x}| \quad &= \sum_{\substack{p_1p_2\in A_x \\ p_1\equiv p_2\equiv 1 \bmod 8}} \frac{1}{32}\Big(1+\Big(\frac{p_1}{p_2}\Big)\Big)\Big(1+\Big(\frac{2p_1}{p_2}\Big)_4\Big)\Big(1+\Big(\frac{2p_2}{p_1}\Big)_4\Big) \\ &\qquad \times\Big(1+\Big(\frac{2}{p_1p_2}\Big)_4\Big)\Big(1+\Big(\frac{2}{p_1}\Big)_4\Big(\frac{\pi_1}{\pi_2}\Big)\Big) \\ &= \frac{1}{512}\cdot\frac{x\log\log x}{\log x} + o\Big(\frac{x\log\log x}{\log x}\Big). \end{aligned}$$

Hence

$$d_4 = \lim_{x\to\infty} \frac{|A_{4,x}|}{|A_x|} = \frac{1}{128}.$$

□

References

[1] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70.

[2] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, Ser. Pure Math. 8, Would Sci., Singapore 1988.

[3] ———, *On the 4-rank of the tame kernel $K_2(\mathcal{O})$ in positive definite terms*, J. Number Theory **88** (2001), no. 2, 263–282.

[4] F. Gerth III, *Counting certain number fields with prescibed l-class numbers*, J. Reine Angew. Math. **337** (1982), 195–207.

[5] ———, *The 4-class ranks of quadratic fields*, Invent. Math. **77** (1984), no. 3, 489–515.

[6] F. Gerth III and S. W. Graham, *Application of a character sum estimate to a 2-class number density*, J. Number Theory **19** (1984), no. 2, 239–247.

[7] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, Fifth edition, London, 1979.

[8] E. Hecke, *Lecture on the Theory of Algebraic Numbers*, GTM 77, Springer-Verlag, 1981.

[9] J. Hurrelbrink and Q. Yue, *On ideal class groups and units in terms of the quadratic form $x^2 + 32y^2$*, Chinese Ann. Math. Ser. B **26** (2005), no. 2, 239–252.

[10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, GTM 84, Springer-Verlag, 1972.

[11] J. Neukirch, *Class Field Theory*, Springer, Berlin, 1986.

[12] P. Stevenhagen, *Divisibity by 2-powers of certain quadratic class numbers*, J. Number Theory **43** (1993), no. 1, 1–19.

[13] X. Wu and Q. Yue, *8-ranks of class groups of some imaginary quadratic number fields*, Acta Math. Sin. (Engl. Ser.) **23** (2007), no. 11, 2061–2068.

[14] Q. Yue, *On tame kernel and class group in terms of quadratic forms*, J. Number Theory **96** (2002), no. 2, 373–387.

[15] ______, *8-ranks of class groups of quadratic number fields and their densities*, Acta Matematica Sinica (Eng. Ser.), to apppear.

[16] Q. Yue and J. Yu, *The densities of* 4*-ranks of tame kernels for quadratic fields*, J. Reine Angew. Math. **567** (2004), 151–173.

Hwanyup Jung
Department of Mathematics Education
Chungbuk National University
Cheongju 361-763, Korea
E-mail address: hyjung@chungbuk.ac.kr

Qin Yue
Department of Mathematics
Nanjing University of Aeronautics and Astronautics
Nanjing, 210016, P. R. China
E-mail address: yueqin@nuaa.edu.cn